UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

IN THE MATTER OF THE SEARCH OF RESIDENTIAL PROPERTY LOCATED AT 8526 SHACKLEFORD LANE, STRAWBERRY PLAINS, TENNESSEE 37871

Case No. 3:19-MJ-2018

Filed Under Seal

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Sean Wilson, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am Sean Wilson, and I am a Special Agent with the United States Capitol Police ("USCP") where I have served since January 5, 2005. I am currently assigned to the USCP Investigations Division, Threat Assessment Section. I have completed hundreds of hours of training in numerous areas of law enforcement investigation and techniques, including but not limited to the following: the Criminal Investigator Training Program and the Mixed Basic Police Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia; the USCP Containment Emergency Response Team Four Week Basic SWAT School; the Pentagon Force Protection Agency One Week Protective Intelligence Course; and the Metropolitan Police Department Crisis Intervention Officer Training Course. In the course of my employment as a Special Agent with the USCP, I have received training regarding the application for and execution of both search and arrest warrants. I have received training in assessing and managing individuals who have communicated threats and engaged in behaviors associated with targeted violence. In my current assignment, I have participated in and conducted numerous investigations involving illegal activity including stalking and threatening communications, both

locally and interstate. As a federal law enforcement officer, I am authorized to execute search and seizure warrants under Rule 41 of the Federal Rules of Criminal Procedure.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. I submit the facts in this affidavit establish probable cause that evidence, fruits, or instrumentalities, specifically described in Attachment B, of violations of 18 U.S.C. § 115(a)(1)(B)—(Influencing Federal Official by Threat) and 18 U.S.C. 875(c)—(Interstate Communication of Threat) will be found in the premises of residential property located at 8526 Shackleford Lane, Strawberry Plains, TN 37871-1008, hereinafter "Premises," more fully described in Attachment A.

JURISDICTION

4. This Court has jurisdiction to issue the requested warrant because the property to be searched is physically located within the Court's district, pursuant to Rule 41(b)(1) of the Federal Rules of Criminal Procedure.

PROBABLE CAUSE

5. On January 31, 2019, Special Agents with the Federal Bureau of Investigation ("FBI") in New York contacted USCP Threat Assessment Section and provided a report from a private citizen regarding a threatening post on the website, www.4chan.org ("4chan.org"), directed at an elected member of the U.S. House of Representatives, hereinafter "U.S.

Congresswoman 1." The FBI Special Agent provided a screenshot of the post which began with a photo of U.S. Congresswoman 1 and stated the following:[1]

> I want all of you to know that 2 weeks i will be trying my best to murder and rape this fucking whore, no i am not a nazi, but this fucking cunt deserves to get raped murdered sodomized tortured and her corpse hung for me to shit on every day. Fucking whore will die soon mark my words this cunt needs to die and get raped by my massive fucking cock she will choke to death on my massive throbbing veiny cock. Fuck conservatives and fuck liberals and fuck this bitch in particular. anyway check in on the news in the next few weeks. >tldr im going to rape, sodomize and murder this dumb cunt

6. I accessed the 4chan.org website and discovered that the post was numbered 789756988 and was created on January 11, 2019, at 2318hrs EST. I took a screen shot of the post which I provided along with the post information to 4chan.org and requested any records connected to the post.

7. An Internet Protocol ("IP") address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. The records provided by 4chan.org showed the post originated from IP address 75.106.229.229.

8. An internet search revealed that this IP address is registered to ViaSat, Inc., a communications company based in Carlsbad, California.

9. I provided the IP address, date, and time of the post to Viasat, Inc. and requested records associated with the IP address.

[1] This quote contains a number of grammar and punctuation errors originally made by the author of the post who is quoted without the use of "sic."

10. The records provided by Viasat, Inc. show that on January 11, 2019, this IP address was in use at the Premises. The records also showed that the customer associated with the Premises is Shawne Huff and the service provided is Fixed Satellite Residential Internet Service.

11. Property records for the Premises show that the Premises is a single family home owned by Shawne Huff and Rebecca Huff.

12. Based on the foregoing, there is probable cause to believe that an electronic device was used to access the internet from the Premises on January 11, 2019, and to create the post which contained the threat to U.S. Congresswoman 1, quoted above in paragraph 5. Therefore, I submit that there is probable cause to search the Premises for evidence, fruits, or instrumentalities of violations of 18 U.S.C. 115(a)(1)(B)—(Influencing Federal Official by Threat) and 18 U.S.C. 875(c)—(Interstate Communication of Threat). I further assert there is probable cause that evidence, fruits, or instrumentalities of these crimes will be contained in electronic devices such as computers that are within the Premises to be searched.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

13. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Premises, in whatever form they are found. One form in which the records might be found is data stored on an electronic device or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

14. *Probable cause.* I submit that if a computer or storage medium is found on the Premises, there is probable cause to believe those records will be stored on that electronic device or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, an electronic device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, electronic device storage media—in particular, electronic devices' internal hard drives—contain electronic evidence of how an electronic has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Electronic device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

15. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronic device files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how electronic devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any electronic storage medium in the Premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the electronic device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within an electronic device and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling law enforcement to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within an

electronic device or electronic storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the electronic device or electronic storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the electronic device was remotely accessed, thus inculpating or exculpating the owner of the electronic device. Further, electronic device and storage media activity can indicate how and when the electronic device or storage media was accessed or used. For example, as described herein, electronic devices typically contain information that log: user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the electronic device accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within an electronic device or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone

with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within an electronic device may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information within the electronic device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw conclusions about how the devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how an electronic device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or

absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses an electronic device to communicate a threat over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain data that is evidence of how the computer was used, data that was sent or received, notes as to how the criminal conduct was achieved, records of Internet discussions about the crime, and other records that indicate the nature of the offense.

16. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the electronic device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing

evidence of how an electronic device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Electronic devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the

warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

18. Because several people may share the Premises as a residence, it is possible that the Premises will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those electronic devices or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

19. Based on the foregoing, I submit that this affidavit supports probable cause for a warrant to search the Premises described in Attachment A and seize the items described in Attachment B. As described herein, it is likely that law enforcement agents executing the warrant will locate electronic devices that contain evidence, fruits, or instrumentalities described in the warrant. Because forensic examiners will be conducting their search of the electronic devices in a law enforcement setting over a prolonged period of time, I respectfully submit good cause has been shown, and therefore request authority, to conduct the search of any electronic devices (or images thereof) seized pursuant to this warrant at any time of the day or night.

REQUEST FOR SEALING

20. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to the target of the investigation. Accordingly, there is good cause to seal these documents because

their premature disclosure may give the target an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Sean Wilson
Special Agent
United States Capitol Police

Subscribed and sworn to before me on this 7th day of February, 2019.

United States Magistrate Judge

ATTACHMENT A

PROPERTY TO BE SEARCHED

The property to be searched is residential property located at 8526 Shackleford Lane, Strawberry Plains, TN 37871-1008, further described as a two-story single family residence with mostly brick exterior, stone lined front stairs and entry, white siding, a gray roof, and a wooden deck to the left of the entry. The property is pictured below.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. All records, documents, programs, applications and information relating to violations of 18 U.S.C. § 115(a)(1)(B)—(Influencing Federal Official by Threat) and 18 U.S.C. § 875(c)—(Interstate Communication of Threat), (collectively, the "Subject Offenses"), including:

a. All records, documents, programs, applications, and information reflecting or relating to any intent, motive, or means of committing violations of the Subject Offenses;

b. All records, documents, programs, applications, and information reflecting any usernames, monikers, and social media and email accounts used to commit violations of the Subject Offenses;

c. All records, documents, programs, applications, and information reflecting the intent or capacity to harm any person or carry out any threats against any person or property;

d. Any and all records, books, magazines, videos, and related correspondence, in whatever form, including handwritten and computer-generated, pertaining to attacks on persons and/or property;

e. Any and all photographs of weapons, ammunition, Senators, Congressmen/Congresswomen, federal facilities, or residences of the foregoing;

f. Indicia of occupancy, residency, and/or ownership of the Premises to be searched;

g. Firearms and ammunition;

h. Electronic devices used to facilitate violations of the Subject Offenses, including but not limited to, computers, routers, modems, hard drives, flash drives, thumb drives, cell phones, tablets, printers, and label making devices;

i. Information and/or data stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer or with the aid of computer-related equipment that was used to facilitate violations of the Subject Offenses. This media includes floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser discs, video cassettes, and other media that is capable of storing magnetic coding, as well as punch cards, and/or paper tapes, and all printouts of stored data;

j. Electronic devices that are capable of analyzing, creating, displaying, converting or transmitting electronic or magnetic computer data that were used to facilitate violations of the Subject Offenses. These devices include computers, computer components, computer peripherals, word-processing equipment, modems, monitors, cables, printers, plotters, encryption circuit boards, optical scanners, external hard drives, external tape backup drives, and other computer-related electronic devices;

k. Any and all instructions or programs stored in the form of electronic or magnetic media that are capable of being interpreted by a computer or related components. The items to be seized include operating systems, application software, utility programs, compilers, interpreters and other programs or software used to communicate with computer hardware or peripherals either directly or indirectly via telephone lines, radio, or other means of transmission; and

l. Any and all written or printed material that provides instruction or examples concerning the operation of computer systems or software, and/or any related device, and sign-on passwords, encryption codes or other information needed to access the computer system and/or software programs.

2. With respect to any electronic device used to facilitate the violations of the Subject Offenses or containing evidence falling within the scope of the foregoing categories of items to be seized:

a. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, monikers, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. Evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. Evidence of the presence or absence of computer software, hardware, or other application, which allows for anonymization of usage on a computer device, including Tor, Virtual Private Networks, VMWare, VirtualBox, multiple boot capabilities, virtualization/virtual machine software, and drive cleaning/wiping software;

d. Evidence of the presence or absence of encryption software, hardware, or other application;

e. Any evidence of Internet research or communications regarding anonymization tools, encryption methods, virtual currency, and virtual currency trading platforms;

f. Any evidence of Internet searches or communications regarding the firearms and destructive devices, including any negotiations or purchases of such items;

g. Evidence of the attachment of other devices;

h. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

i. Evidence of the times the device was used;

j. Passwords, encryption keys, and other access devices that may be necessary to access the device;

k. Applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

l. Records of or information about Internet Protocol addresses used by the device; and

m. Records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

II. SEARCH PROCEDURE FOR ELECTRONIC DEVICES

1. In searching the electronic devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any electronic device capable of being used to facilitate violations of the Subject Offenses or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each electronic device where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location. Members of the search team may also access the electronic devices remotely.

c. The search team shall complete the search of the electronic devices as soon as is practicable, but not to exceed 120 days from the date of issuance of the warrant. The government will not search the electronic device(s) beyond this 120-day period without first obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each electronic device capable of containing any of the items to be seized to the search protocols to determine whether the electronic device and any data therein falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. If the search team, while searching an electronic device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the search team shall immediately discontinue its search of that electronic device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

f. If the search team determines that an electronic device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the electronic device and delete or destroy all forensic copies thereof.

g. If the search team determines that an electronic device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search team determines that the electronic device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the electronic device, but may not access data

falling outside the scope of the items to be seized (after the time for searching the device has expired) absent further order of the Court.

i. The government may retain an electronic device itself until further order of the Court or one year after the conclusion of the criminal investigation or case, only if the electronic device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the electronic device (or while an application for such an order is pending). Otherwise, the government must return the electronic device.

j. After the completion of the search of the electronic devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

2. The special procedures relating to electronic devices found in this warrant govern only the search of electronic devices pursuant to the authority conferred by this warrant and do not apply to any search of electronic devices pursuant to any other order of the Court.